REMARKS/ARGUMENTS

Status of Claims

Claims 21-31 are pending in this application, with claims 21, 25, 27, and 29 being independent. Claims 21, 23, and 25-31 have been amended.

Summary of Substance of Interview

Applicants would like to thank the Examiner for conducting a telephonic interview on June 18, 2010. As indicated in the Interview Summary dated July 8, 2010, agreement was reached that cited reference Chaudary does not disclose all of the elements of claim 21. It is believed that the Examiner's Interview Summary in conjunction with the remarks made herein adequately summarize the substance of the interview, in accordance with M.P.E.P. § 713.04.

Overview of the Office Action

Claims 21, 25, 27, and 29 have been rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Claims 21-31 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. 7,155,526 ("Chaudhary").

Rejections Under 35 U.S.C. § 112

The Office Action states that the claims lack written description support, because they are purportedly directed to two individual users, rather than a single user. However, the terms "first user identifier" and "second user identifier" define two <u>user identifiers</u> associated with a single user, as described throughout the specification, rather than two <u>users</u>, each having an identifier. Nevertheless, the claims have been amended, as discussed during the interview, to recite "a first identifier" and a "second identifier" to address the Examiner's concerns in this regard.

Accordingly, it is deemed that these rejections have been overcome. Withdrawal of these rejections is therefore requested.

The Examiner stated during the interview that in claim 21, the phrase "calculated using at least one predefined cryptographic algorithm applied to the random number received and at least one secret key specific to the user" was possibly indefinite, because it was supposedly unclear whether the cryptographic algorithm is applied to the random number alone or whether it is applied to both the random number and the secret key. The specification discloses that the cryptographic algorithm is applied to the random number <u>using</u> the user's secret key. Accordingly, Claim 21 has been amended based on page 13, lines 7-9, of the specification. The phrase in question now reads: "calculated by applying at least one predefined cryptographic algorithm to the received random number using at least one secret key specific to the user." It is deemed that the amended phrase would be readily understood by one of ordinary skill in the art.

In addition, the Examiner questioned during the interview whether the specification discloses a correspondence between the claimed identifiers (e.g., "ID1" and "ID2") and the claimed entities (e.g., the access provider and the service provider). The Examiner agreed that the specification discloses a correspondence between the claimed passwords and the entities, but he stated that he did not think a correspondence is disclosed for the identifiers. This discussion was related to the portion of claim 21 reciting: "the access controller transmits, to each of the authentication devices for the first and second entities, a respective authentication request containing (i) the first user identifier data and the first password for the first entity, and (ii) the second user identifier data and the second password for the second entity."

In response to the Examiner's concerns, Applicants note that the specification states at page 13, lines 26-30 (emphasis added): "[t]his request message 44 includes identifiers ID1 and

ID2 for identifying the user, respectively, to the selected access and service provider." Applicants respectfully submit that as a matter of ordinary English grammar, the phrase "A and B for identifying the user, respectively, to X and Y" means that element A identifies the user to element X, and element B identifies the user to element Y. Thus, this cited portion establishes a correspondence between the identifiers and the entities.

Furthermore, the specification, at page 14, lines 14-26, states (emphasis added):

> In the next step 27, the access controller receives the request 45 and extracts the identification and authentication parameters therefrom. These parameters are transmitted in steps 28, 29 in authentication messages 46, 47, respectively, to the authentication servers 16 of the selected access provider and service provider. The identification information ID1 and ID2 is, for example, in the form "IdA@domainA," wherein "IdA" enables the user to be uniquely identified to the access or service provider, and "domainA" makes it possible to determine the domain name, in the IP network, of the server to which the corresponding authentication message is to be sent.

It is clear from this cited portion that the identifiers each correspond to a particular entity. Therefore, it is deemed that the specification provides more than adequate support for the elements of claim 21 discussed above.

Summary of Subject Matter Disclosed in the Specification

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

The embodiments disclosed in the present application relate to methods and systems for authenticating a user to multiple entities in a data transmission network. In conventional systems, when a user wishes to connect to a network service, the user must first connect to the IP network by performing authentication with an access provider and then performing a second authentication with the service provider (e.g., an online banking service). This requires a user to make multiple authentications to access desired services. The disclosed embodiments allow authentication to be carried out for more than one independent network entity based on a single authentication procedure. (Specification at page 2, line 6 – page 3, line 12).

To access an IP service using the disclosed methods, the user terminal (11) first establishes a connection with a specialized server (12). A random number (RAND) is sent to the user terminal (11) by the specialized server (12). The user terminal (11) may transmit the random number to a module (15) attached to the terminal, e.g., a SIM card. The module (15) applies a cryptographic algorithm to the random number using a secret key of the user to obtain a password for user authentication to an entity in the network. A separate password (e.g., AUTH1, AUTH2) is generated in this manner for each entity to be accessed and transmitted by the module (15) back to the user terminal (11). (Page 12, line 4 – page 13, line 20).

The user terminal (11) sends an access request message to the specialized terminal (12) including an identifier (e.g., ID1, ID2) to identify the user to each of the entities to which authentication is desired and the corresponding passwords (e.g., AUTH1, AUTH2) for each entity. The specialized server (12) encapsulates this message in a conventional authorization request format, such as a remote authentication dial-in user service (RADIUS) format. The authorization request includes: a user-name, which may be a concatenation of the identifiers (ID1, ID2) of the entities; a password, which may be a concatenation of the passwords (AUTH1, AUTH2) of the entities; and the random number (RAND) generated earlier by the specialized server (12). The authorization request is then sent by the specialized server (12) to the access controller (10) to obtain access to the IP network. (Page 13, line 24 – page 14, line 13).

The access controller (10) extracts the identifiers and passwords from the authorization request and creates separate authentication messages to be sent to each of the entities (e.g., the access provider and the service provider). The identifiers (ID1, ID2) may be in the form "IdA@domainA" and "IdB@domainB," where "IdA" enables the user to be uniquely identified to the first entity (e.g., the access provider) and "IdB" enables the user to be uniquely identified to the second entity (e.g., the service provider). These separate authentication messages each contain the identifier and password corresponding to the recipient entity, as well as the random number (RAND). (Page 14, lines 14-30).

Upon receipt of an authentication message, an authentication server (16) of the entity carries out an authentication procedure that involves identifying the user via the identifier (ID1, ID2); retrieving a secret key of the user from a database; and calculating a password for the user using the secret key and the random number (RAND). The password is calculated using the same cryptographic algorithm as that used by the module (15) connected to the user terminal (11), as described above. The calculated password is then compared to the password received in the received authentication message. This process is performed at each entity, e.g., the access provider and the service provider, and the results of the authentication are reported back to the access controller 10 to complete the authentication process. (Page 14, line 31 – page 15, line 28).

<u>Descriptive Summary of the Prior Art</u>

Chaudary relates to systems and methods for integrating a wireless local area network (WLAN) into a GSM/GPRS core network, wherein gateways are added that transparently transport services between the two networks. As depicted in Fig. 3 of Chaudary, the system has two network elements, a radio link manager (RLM) and a radio access controller (RAC), and also has a software application, the "multi-link client" (MLC), to control the functionality of the integration and the authentication. The MLC resides on a user device. The RAC provides protocol stacks and interworking functions to allow the MLC to talk to a home location register (HLR). The RLM and MLC set up a tunnel employing, for example, PPP over ethernet (PPPOE), and all of the data packets received on this tunnel are forwarded by the RLM to the gateway GPRS support node (GGSN) over a further tunnel using the GPRS tunneling protocol (GTP). The GGSN, in turn, provides access to the internet. (Chaudary, Abstract and Fig. 3).

Patentability over the Prior Art

Chaudary, as discussed above, provides a way for a wireless LAN to connect to the internet through the mobile/cellular network (i.e., a GSM/GPRS network). As agreed during the interview, Chaudary does not teach or suggest a method for enabling a user to be authenticated to two entities, but is merely concerned with mutual authentication between a wireless LAN and a mobile/cellular network gateway. It is clear from a review of Chaudary that this reference does not teach or suggest, for example, that "a distinct set of data for each of a first entity and a second entity for authenticating the user to both the first and the second entities of the network is calculated by applying at least one predefined cryptographic algorithm to the received random number using at least one secret key specific to the user, wherein the distinct set of data comprises (i) a first password for the first entity and (ii) a second password for the second entity," as recited in claim 21.

A fortiori, Chaudary does not teach or suggest that "the terminal inserts, in an access request, first user identifier data and second user identifier data for identifying the user to said first and second entities of the network and the two distinct sets of data," as further recited in claim 21. The Office Action cited column 10, lines 20-35, of Chaudary in this regard. However, as discussed during the interview, this cited portion relates to an authentication request formed by the HLR and sent to the terminal, rather than a request formed by the terminal, in the manner recited in claim 21.

In view of the above, claim 21 is deemed to be patentable over Chaudary.

Independent claims 25, 27, and 29, as amended, recite features similar to claim 21 and are therefore also deemed to be patentable over the applied prior art for reasons discussed above with respect to claim 21.

Claims 22-24, 26, 28, and 30-31, which each depend from one of independent claims 21, 25, 27, and 29, distinguish the invention over the applied prior art for reasons discussed above in regard to the independent claims as well as on their own merits.

Conclusion

Based on all of the above, the present application is now in proper condition for allowance. Prompt and favorable action to this effect and early passing of this application to issue are respectfully solicited.

It is believed that no additional fees or charges are required at this time in connection with the present application. However, if any additional fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Carl B. Wischhusen/
Carl B. Wischhusen
Reg. No. 43,279
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: July 19, 2010